UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/615,882	07/08/2003	Philip Michael Hawkes	030441	9835

23696   7590   03/30/2010
QUALCOMM INCORPORATED
5775 MOREHOUSE DR.
SAN DIEGO, CA 92121

EXAMINER
SIMITOSKI, MICHAEL J

ART UNIT	PAPER NUMBER
2439	

NOTIFICATION DATE	DELIVERY MODE
03/30/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

us-docketing@qualcomm.com
kascanla@qualcomm.com
nanm@qualcomm.com

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 January 2010*.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *64-86* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *64-86* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *17 September 2007* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

        1.☐ Certified copies of the priority documents have been received.

        2.☐ Certified copies of the priority documents have been received in Application No. _____.

        3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application

6)☐ Other: _____ .

DETAILED ACTION

1.   The response of 1/7/2010 was received and considered.

2.   Claims 64-86 are pending.

Response to Arguments

3.   Applicant's arguments filed 1/7/2010 have been fully considered but they are not persuasive.

 a.   Applicant's response (p. 10) argues that Ahonen and Hawkes fail to teach the amended limitations, namely (1) that the private key is not accessible to the mobile equipment, (2) the secure processing unit provides more secure key storage than the mobile equipment and (3) the secure processing unit has processing power sufficient to decrypt a broadcast access key and generate a short term key, but not to decrypt multimedia content. However, Hawkes discloses that (regarding (1)), the private key (RK) is not accessible to the mobile equipment (RK is not provided to the ME, ¶72), (regarding (2)), the secure processing unit provides more secure key storage than the mobile equipment (SUMU has a secure memory unit, ¶65, storing an A-key, ¶72 an RK, ¶72 and SK, ¶78, whereas the ME only stores the SK, ¶78) and (regarding (3)), the secure processing unit (SUPU) has processing power to decrypt a broadcast access key and a short term key (UIM is able to recover the value of BAK, ¶70 and able to able to compute SK, ¶73), but not to decrypt multimedia content (SUPU does not have significant processing power for functions beyond security and key procedures such as to allow encryption of the broadcast content of the HSBS, ¶66). Therefore, the amended limitations are disclosed in at least Hawkes.

Claim Objections

4.   Claims 72-81 are objected to because of the following informalities:

b.   Regarding claim 72, lines 4-5, the limitation "securing storing" is believed to read

"securely storing".

c.   Regarding claim 77, lines 5-6, the limitation "secure processing unit provides more

secure key storage than the secure processing unit" is believed to read "secure processing unit

provides more secure key storage than the mobile equipment".

d.   Regarding claims 77-81, the preamble "machine readable medium" should recite instead

"a non-transitory machine-readable medium" such that it is understood the claim does not include

transitory mediums. The broadest reasonable interpretation of a claim drawn to a computer

readable medium (also called machine readable medium and other such variations) typically

covers forms of non-transitory tangible media and transitory propagating signals per se in view of

the ordinary and customary meaning of computer readable media, particularly when the

specification is silent. See MPEP §2111.01. A claim drawn to such a computer readable medium

that covers both transitory and non-transitory embodiments may be amended to narrow the claim

to cover only statutory embodiments to avoid a rejection under 35 U.S.C. §101 by adding the

limitation "non-transitory" to the claim. Such an amendment would typically not raise the issue

of new matter, even when the specification is silent because the broadest reasonable interpretation

relies on the ordinary and customary meaning that includes signals per se. Further, an

amendment to the specification to provide sufficient antecedent basis for the claim terminology,

such as "non-transitory" may be necessary and would not typically raise the issue of new matter.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

5.   The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the
subject matter which the applicant regards as his invention.

6.   Claims 64-71 and 77-81 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite

for failing to particularly point out and distinctly claim the subject matter which applicant regards as the

invention.

        e.   Regarding claims 64-71 and 77-81, the claims as amended, include limitations directed to

        the processing power or memory size of the respective components. However, it is unclear how

        or if these limitations have any effect on the scope of the method or machine readable medium

        claims, respectively.

Claim Rejections - 35 USC § 103

7.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness

rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of
> this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as
> a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said
> subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8.   Claims 64-69, 71-75, 77-80 & 82-85 are rejected under 35 U.S.C. 103(a) as being unpatentable

over U.S. Patent Application Publication 2002/0141591, published 11/3/2002 to Hawkes et al. (**Hawkes**)

in view of U.S. Patent Application Publication 2006/0168446 to Ahonen et al. (**Ahonen**).

        Regarding claim 64, Hawkes discloses a method for broadcasting encrypted multimedia content

from a content provider (content server, ¶63) to a plurality of authorized terminals (MS) over the air

(¶57), comprising each terminal having a mobile equipment (ME, Fig. 4, #306) and having a secure

processing unit (UIM, Fig. 4, #308) that securely stores a unique key (RK is stored in SUMU, Fig. 4,

#314, ¶74), such that the unique private key is not accessible to the mobile equipment of the respective

terminal (SUMU discourages unauthorized access to the information, ¶65 and RK is not provided to the

ME, ¶72), the secure processing unit provides more secure key storage than the mobile equipment

(SUMU has a secure memory unit, ¶65, storing an A-key, ¶72 an RK, ¶72 and SK, ¶78, whereas the ME

only stores the SK, ¶78), the secure processing unit (SUPU) has processing power sufficient to decrypt a

broadcast access key and to generate a short term key (UIM is able to recover the value of BAK, ¶70 and

able to able to compute SK, ¶73) and the secure processing unit does not have processing power sufficient

to decrypt multimedia content (SUPU does not have significant processing power for functions beyond

security and key procedures such as to allow encryption of the broadcast content of the HSBS, ¶66) and

the broadcast access key (BAK) is encrypted by the content provider using the unique keys (RK) of each

of the respective terminals to authorize the respective terminal to receive the encrypted multimedia

content (BAK is encrypted with RK, ¶74), each terminal receiving the respective encrypted broadcast

access key (BAK) over the air from the content provider (BAKI is received from CS, ¶74) and providing

the respective encrypted broadcast access key (BAKI is passed to the UIM, ¶74) to the terminal's secure

processing unit (UIM, ¶74), wherein the terminal's secure processing unit (UIM) decrypts the encrypted

broadcast access key (BAKI) using the secure processing unit's unique key (RK is used in the UIM to

decrypt BAK from BAKI, ¶74) and securely stores the broadcast access key (BAK is stored in SUMU,

¶74), each terminal receiving short-term key information (SKI, ¶76 & ¶78) and encrypted multimedia

content (received broadcast content, ¶80) over the air from the content provider (CS) to the terminals

(MS, ¶76 & ¶80), wherein the content is encrypted with a short-term key (¶81), and wherein the short-

term key is generated using the broadcast access key (BAK) and short-term key information (SKI and

BAK are processed to determine SK, ¶76), and provides the short-term key (SK) to the terminal's mobile

equipment (SK is passed to ME, ¶¶80-81, last two lines of each), and each terminal's mobile equipment

decrypting the multimedia content using the short-term key (ME decrypts the received broadcast content,

¶¶80-81, last two lines of each). Hawkes lacks each terminals forwarding a unique public key over the air

to the content provider and lacks wherein the secure processing unit stores a unique private key (instead

of Hawkes's RK), corresponding to the unique public key. However, Ahonen teaches a system where a

terminal forwards a unique public key over the air (over a 3G network, ¶37) to a content provider

(terminal sends a registration message to a group controller, the message including a copy of the terminal's public key, ¶38), wherein each terminal stores a unique private key corresponding to the unique public key (terminal creates a signature using the private key, ¶38 & ¶42, showing that the terminal stores the private key). Similarly to Hawkes's RK, the private key that corresponds to the forwarded unique public key in Ahonen is used to decrypt a received encrypted key encrypting key (KEK), which is similar to Hawkes's BAK (¶41). The KEK is then used to decrypt a received encrypted traffic encrypting key (TEK, ¶41) which decrypts the broadcast content (¶36) that is received, possibly from the group controller (¶19). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Hawkes such that each terminal (MS) forwards a unique public key over the air to the content provider (CS), wherein the secure processing unit (UIM) stores a unique private key (instead of Hawkes's RK), corresponding to the unique public key. One of ordinary skill would have been motivated to perform this modification to achieve a simple mechanism for key dissemination, as taught by Ahonen (¶7). One of ordinary skill in the art at the time the invention was made would appreciate this benefit because Ahonen is using the existing, well-known, public key infrastructure to share a key, rather than a more complex protocol such as AKA or IKE.

Regarding claim 65, Hawkes, as modified above, discloses wherein the short-term key (SK) is accessible to a user (Hawkes discloses that data in the ME is easily accessed, ¶64 and that SK is passed to the ME for decrypting of the broadcast content, ¶78; therefore, the SK is accessible to a user).

Regarding claim 66, Hawkes, as modified above, discloses wherein the short-term key is changed by the content provider at a rate such that the cost of an unauthorized terminal user obtaining the short-term key from the mobile equipment exceeds the value of the short-term key to the unauthorized terminal user (Hawkes discloses that the SK is changed frequently such that the cost of a non-subscriber obtaining SK form the memory exceeds the value of SK, ¶68).

Regarding claim 67, Hawkes, as modified above, discloses wherein the secure processing unit (UIM) is removable from the terminal (¶66).

Regarding claim 68, Hawkes, as modified above, discloses wherein the short-term key information (SKI) is the short-term key encrypted using the broadcast access key (SKI may be the encryption of SK using BSK as the key, ¶76).

Regarding claim 69, Hawkes, as modified above, discloses wherein the short-term key (SK) is generated by applying a cryptographic hash to a concatenation of the short-term key information (SKI) and the broadcast access key (BAK, ¶76, last three lines).

Regarding claim 71, Hawkes, as modified above, discloses wherein at least one terminal (MS) comprises a mobile station (Fig. 3, #206 & ¶57).

Regarding claim 72, Hawkes discloses an integrated circuit (¶107) for a mobile station (MS, Fig. 4, #300) comprising means for securely storing a unique key (RK is stored in SUMU, Fig. 4, #314, ¶74) such that the unique key is not accessible to a user (SUMU discourages unauthorized access to the information, ¶65 and RK is not provided to the ME, ¶72), wherein the means for securely storing (SUPU) has processing power sufficient to decrypt a broadcast access key and to generate a short term key (UIM is able to recover the value of BAK, ¶70 and able to able to compute SK, ¶73), and does not have processing power sufficient to decrypt multimedia content (SUPU does not have significant processing power for functions beyond security and key procedures such as to allow encryption of the broadcast content of the HSBS, ¶66) and wherein the content provider (CS) encrypts a broadcast access key (BAK) with each of the unique keys (RK) to authorized an integrated circuit securely storing a corresponding key to receive the encrypted multimedia content (BAK is encrypted with RK, ¶74 and RK is stored in the UIM, ¶74), means (MS) for receiving the respective encrypted broadcast access key (BAK) over the air from the content provider (BAKI is received from CS, ¶74), means (MS) for decrypting the encrypted broadcast access key (BAKI) using the secure processing unit's unique key (RK is used in the UIM to

decrypt BAK from BAKI, ¶74) and securely storing the broadcast access key (BAK is stored in SUMU,

¶74), wherein the securely stored broadcast access key is not accessible to a user (SUMU discourages

unauthorized access to the information, ¶65 and the BAK is stored in the SUMU, ¶74), means (MS) for

receiving short-term key information (SKI, ¶76 & ¶78) and encrypted multimedia content (received

broadcast content, ¶80) over the air from the content provider (CS) to the a plurality of mobile stations

(Fig. 3, #206) each having the integrated circuit (MS, ¶76 & ¶80, Fig. 4, #300), wherein the content is

encrypted with a short-term key (¶81), and wherein the short-term key is generated using the broadcast

access key (BAK) and short-term key information (SKI and BAK are processed to determine SK, ¶76),

means (MS) for generating the short term key using the securely stored broadcast access key (BAK) and

the broadcast short-term key information (SKI and BAK are processed to determine SK, ¶76) and means

(MS) for decrypting the multimedia content using the short-term key (ME decrypts the received broadcast

content using SK, ¶¶80-81, last two lines of each), wherein the means for securely storing provides more

secure key storage than the means for decrypting the multimedia content (SUMU has a secure memory

unit, ¶65, storing an A-key, ¶72 an RK, ¶72 and SK, ¶78, whereas the ME only stores the SK, ¶78).

Hawkes lacks forwarding a unique public key over the air to the content provider and lacks securely

storing a unique private key (instead of Hawkes's RK), corresponding to the unique public key.

However, Ahonen teaches a system where a terminal forwards a unique public key over the air (over a 3G

network, ¶37) to a content provider (terminal sends a registration message to a group controller, the

message including a copy of the terminal's public key, ¶38), wherein each terminal stores a unique

private key corresponding to the unique public key (terminal creates a signature using the private key, ¶38

& ¶42, showing that the terminal stores the private key). Similarly to Hawkes's RK, the private key that

corresponds to the forwarded unique public key in Ahonen is used to decrypt a received encrypted key

encrypting key (KEK), which is similar to Hawkes's BAK (¶41). The KEK is then used to decrypt a

received encrypted traffic encrypting key (TEK, ¶41) which decrypts the broadcast content (¶36) that is

received, possibly from the group controller (¶19). Therefore, it would have been obvious to one having

ordinary skill in the art at the time the invention was made to modify Hawkes's terminal such that each

terminal (MS) forwards a unique public key over the air to the content provider (CS), wherein the secure

processing unit (UIM) stores a unique private key (instead of Hawkes's RK), corresponding to the unique

public key. One of ordinary skill would have been motivated to perform this modification to achieve a

simple mechanism for key dissemination, as taught by Ahonen (¶7). One of ordinary skill in the art at the

time the invention was made would appreciate this benefit because Ahonen is using the existing, well-

known, public key infrastructure to share a key, rather than a more complex protocol such as AKA or

IKE.

Regarding claim 73, Hawkes, as modified above, discloses wherein the short-term key (SK) is

accessible to a user (Hawkes discloses that data in the ME is easily accessed, ¶64 and that SK is passed to

the ME for decrypting of the broadcast content, ¶78; therefore, the SK is accessible to a user).

Regarding claim 74, Hawkes, as modified above, discloses wherein the short-term key

information (SKI) is the short-term key encrypted using the broadcast access key (SKI may be the

encryption of SK using BSK as the key, ¶76).

Regarding claim 75, Hawkes, as modified above, discloses wherein the short-term key (SK) is

generated by applying a cryptographic hash to a concatenation of the short-term key information (SKI)

and the broadcast access key (BAK, ¶76, last three lines).

Regarding claim 77, Hawkes discloses a machine-readable medium (¶108) comprising code for

securely storing a unique key (RK is stored in SUMU, Fig. 4, #314, ¶74), in a secure processing unit of a

terminal (UIM) such that the unique key is not accessible to a mobile equipment of the terminal (SUMU

discourages unauthorized access to the information, ¶65 and RK is not provided to the ME, ¶72), wherein

the secure processing unit provides more secure key storage than the mobile equipment (SUMU has a

secure memory unit, ¶65, storing an A-key, ¶72 an RK, ¶72 and SK, ¶78, whereas the ME only stores the

SK, ¶78), wherein the secure processing unit (SUPU) has processing power sufficient to decrypt a

broadcast access key and to generate a short term key (UIM is able to recover the value of BAK, ¶70 and

able to able to compute SK, ¶73), but does not have processing power sufficient to decrypt multimedia

content (SUPU does not have significant processing power for functions beyond security and key

procedures such as to allow encryption of the broadcast content of the HSBS, ¶66) and wherein the

broadcast access key is encrypted by the content provider (CS) using the unique keys (RK) to authorize

the respective terminal to receive the encrypted multimedia content (BAK is encrypted with RK, ¶74 and

RK is stored in the UIM, ¶74), code (MS, ¶108) for receiving the respective encrypted broadcast access

key (BAK) over the air from the content provider (BAKI is received from CS, ¶74), code (MS, ¶108) for

decrypting the encrypted broadcast access key (BAKI) using the secure processing unit's unique key (RK

is used in the UIM to decrypt BAK from BAKI, ¶74) and securely storing the broadcast access key (BAK

is stored in SUMU, ¶74), wherein the securely stored broadcast access key is not accessible to a user

(SUMU discourages unauthorized access to the information, ¶65 and the BAK is stored in the SUMU,

¶74), code (MS, ¶108) for receiving short-term key information (SKI, ¶76 & ¶78) and encrypted

multimedia content (received broadcast content, ¶80) over the air from the content provider (CS) to the a

plurality of terminals (Fig. 3, #206) each having a integrated circuit (MS, ¶76, ¶80 & ¶107, Fig. 4, #300),

wherein the multimedia content is encrypted with a short-term key (¶81), and wherein the short-term key

is generated using the broadcast access key (BAK) and short-term key information (SKI and BAK are

processed to determine SK, ¶76), code (MS, ¶108) for generating the short term key using the securely

stored broadcast access key (BAK) and the broadcast short-term key information (SKI and BAK are

processed to determine SK, ¶76) and code (MS, ¶108) for decrypting the multimedia content using the

short-term key (ME decrypts the received broadcast content using SK, ¶¶80-81, last two lines of each).

Hawkes lacks forwarding a unique public key over the air to the content provider and lacks securely

storing a unique private key (instead of Hawkes's RK), corresponding to the unique public key.

However, Ahonen teaches a system where a terminal forwards a unique public key over the air (over a 3G network, ¶37) to a content provider (terminal sends a registration message to a group controller, the message including a copy of the terminal's public key, ¶38), wherein each terminal stores a unique private key corresponding to the unique public key (terminal creates a signature using the private key, ¶38 & ¶42, showing that the terminal stores the private key). Similarly to Hawkes's RK, the private key that corresponds to the forwarded unique public key in Ahonen is used to decrypt a received encrypted key encrypting key (KEK), which is similar to Hawkes's BAK (¶41). The KEK is then used to decrypt a received encrypted traffic encrypting key (TEK, ¶41) which decrypts the broadcast content (¶36) that is received, possibly from the group controller (¶19). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Hawkes's terminal such that each terminal (MS) comprises code that forwards a unique public key over the air to the content provider (CS), wherein the terminal includes code for storing securely a unique private key (instead of Hawkes's RK), corresponding to the unique public key. One of ordinary skill would have been motivated to perform this modification to achieve a simple mechanism for key dissemination, as taught by Ahonen (¶7). One of ordinary skill in the art at the time the invention was made would appreciate this benefit because Ahonen is using the existing, well-known, public key infrastructure to share a key, rather than a more complex protocol such as AKA or IKE.

Regarding claim 78, Hawkes, as modified above, discloses wherein the short-term key (SK) is accessible to a user (Hawkes discloses that data in the ME is easily accessed, ¶64 and that SK is passed to the ME for decrypting of the broadcast content, ¶78; therefore, the SK is accessible to a user).

Regarding claim 79, Hawkes, as modified above, discloses wherein the short-term key information (SKI) is the short-term key encrypted using the broadcast access key (SKI may be the encryption of SK using BSK as the key, ¶76).

Regarding claim 80, Hawkes, as modified above, discloses wherein the short-term key (SK) is

generated by applying a cryptographic hash to a concatenation of the short-term key information (SKI)

and the broadcast access key (BAK, ¶76, last three lines).

Regarding claim 82, Hawkes discloses an apparatus (MS, Fig. 4, #300) for receiving encrypting

multimedia content broadcast over the air (Fig. 3, #206) from a content provider (CS, ¶63) to a plurality

of authorized apparatuses (Fig. 3, #206) comprising a mobile equipment (ME, Fig. 4, #306) configured to

decrypt the multimedia content using the short-term key (ME decrypts the received broadcast content

using SK, ¶¶80-81, last two lines of each), wherein the multimedia content is encrypted with the short-

term key (SK, ¶81), and wherein the short-term key is generated using the broadcast access key (BAK)

and short-term key information (SKI and BAK are processed to determine SK, ¶76), and a secure

processing unit (UIM, Fig. 4, #308) configure to securely store a unique key (RK is stored in SUMU, Fig.

4, #314, ¶74) that is not accessible to the mobile equipment (SUMU discourages unauthorized access to

the information, ¶65 and RK is not provided to the ME, ¶72), wherein the secure processing unit provides

more secure key storage than the mobile equipment (SUMU has a secure memory unit, ¶65, storing an A-

key, ¶72 an RK, ¶72 and SK, ¶78, whereas the ME only stores the SK, ¶78), wherein the secure

processing unit (SUPU) has processing power sufficient to decrypt a broadcast access key and to generate

a short term key (UIM is able to recover the value of BAK, ¶70 and able to able to compute SK, ¶73), but

does not have processing power sufficient to decrypt multimedia content (SUPU does not have significant

processing power for functions beyond security and key procedures such as to allow encryption of the

broadcast content of the HSBS, ¶66) and wherein the content provider (CS) encrypts a broadcast access

key (BAK) with the unique key (RK) to authorize an apparatus having the secure processing unit

(authorize the MS) securely storing the corresponding key (RK) to receive the encrypted multimedia

content (BAK is encrypted with RK, ¶74 and RK is stored in the UIM, ¶74), receive the respective

encrypted broadcast access key (BAK) over the air (Fig. 3, #206) from the content provider (BAKI is

received from CS, ¶74), decrypt the encrypted broadcast access key (BAKI; RK is used in the UIM to

decrypt BAK from BAKI, ¶74) and securely store the broadcast access key (BAK is stored in SUMU,

¶74), wherein the securely stored broadcast access key is not accessible to a user (SUMU discourages

unauthorized access to the information, ¶65 and the BAK is stored in the SUMU, ¶74), receive the short-

term key information (SKI) broadcast over the air from the content provider (CS sends SKI to MS, ¶76)

and generate the short-term key using the securely stored broadcast access key (BAK) and broadcast

short-term key information (SKI and BAK are processed to determine SK, ¶76). Hawkes lacks the mobile

equipment forwarding a unique public key over the air to the content provider and lacks the secure

processing unit securely storing a unique private key (instead of Hawkes's RK), corresponding to the

unique public key. However, Ahonen teaches a system where a terminal forwards a unique public key

over the air (over a 3G network, ¶37) to a content provider (terminal sends a registration message to a

group controller, the message including a copy of the terminal's public key, ¶38), wherein each terminal

stores a unique private key corresponding to the unique public key (terminal creates a signature using the

private key, ¶38 & ¶42, showing that the terminal stores the private key). Similarly to Hawkes's RK, the

private key that corresponds to the forwarded unique public key in Ahonen is used to decrypt a received

encrypted key encrypting key (KEK), which is similar to Hawkes's BAK (¶41). The KEK is then used to

decrypt a received encrypted traffic encrypting key (TEK, ¶41) which decrypts the broadcast content

(¶36) that is received, possibly from the group controller (¶19). Therefore, it would have been obvious to

one having ordinary skill in the art at the time the invention was made to modify Hawkes's terminal such

that the mobile equipment (ME) forwards a unique public key over the air to the content provider (CS)

and the secure processing unit (UIM) stores a unique private key (instead of Hawkes's RK),

corresponding to the unique public key. One of ordinary skill would have been motivated to perform this

modification to achieve a simple mechanism for key dissemination, as taught by Ahonen (¶7). One of

ordinary skill in the art at the time the invention was made would appreciate this benefit because Ahonen

is using the existing, well-known, public key infrastructure to share a key, rather than a more complex

protocol such as AKA or IKE.

Regarding claim 83, Hawkes, as modified above, discloses wherein the short-term key (SK) is

accessible to a user (Hawkes discloses that data in the ME is easily accessed, ¶64 and that SK is passed to

the ME for decrypting of the broadcast content, ¶78; therefore, the SK is accessible to a user).

Regarding claim 84, Hawkes, as modified above, discloses wherein the short-term key

information (SKI) is the short-term key encrypted using the broadcast access key (SKI may be the

encryption of SK using BSK as the key, ¶76).

Regarding claim 85, Hawkes, as modified above, discloses wherein the short-term key (SK) is

generated by applying a cryptographic hash to a concatenation of the short-term key information (SKI)

and the broadcast access key (BAK, ¶76, last three lines).

9.   Claims 70, 76, 81 & 86 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Hawkes**

and **Ahonen**, as applied to claims 69, 75, 80 & 85 above, in further view of Applied Cryptography,

Second Edition by Bruce Schneier (**Schneier**).

Regarding claims 70, 76, 81 & 86, Hawkes, as modified above, discloses wherein the short-term

information is at least partly unpredictable, but lacks explicitly where it is a random value. However,

Schneier discloses that good keys for encryption are random, such that all possible values are equally

likely (i.e. unpredictable, p. 173, §Random Keys, ¶1). Therefore, it would have been obvious to one

having ordinary skill in the art at the time the invention was made to modify Hawkes invention, as

modified above, such that the short-term information is a random value. One of ordinary skill in the art

would have been motivated to perform such a modification to enhance the security of the encrypted data

such that the key is unpredictable via its randomness, as taught by Schneier.

Conclusion

10.   Applicant's amendment necessitated the new ground(s) of rejection presented in this Office

action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is

reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

        A shortened statutory period for reply to this final action is set to expire THREE MONTHS from

the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing

date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH

shortened statutory period, then the shortened statutory period will expire on the date the advisory action

is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX

MONTHS from the date of this final action.

        Any inquiry concerning this communication or earlier communications from the examiner should

be directed to MICHAEL J. SIMITOSKI whose telephone number is (571)272-3841. The examiner can

normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m..

        If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Edan

Orgad can be reached on (571)272-7884. The fax phone number for the organization where this

application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application

Information Retrieval (PAIR) system. Status information for published applications may be obtained

from either Private PAIR or Public PAIR. Status information for unpublished applications is available

through Private PAIR only. For more information about the PAIR system, see http://pair-

direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer

Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR

CANADA) or 571-272-1000.

March 24, 2010
/Michael J Simitoski/
Primary Examiner, Art Unit 2439